



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.   | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.                  | CONFIRMATION NO.       |
|---|-------------|----------------------|--------------------------------------|------------------------|
| 10/796,599  | 03/09/2004  | Weishi Feng          | MP0386                               | 1797                   |
| 26703 7590 09/14/2007<br>HARNESS, DICKEY & PIERCE P.L.C.<br>5445 CORPORATE DRIVE<br>SUITE 200<br>TROY, MI 48098 |             |                      | EXAMINER<br>SAN JUAN, MARTINJERIKO P |                        |
|   |             |                      | ART UNIT<br>2132                     | PAPER NUMBER           |
|   |             |                      | MAIL DATE<br>09/14/2007              | DELIVERY MODE<br>PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

Application No.

10/796,599

Applicant(s)

FENG, WEISHI

Examiner

Martin Jeriko P. San Juan

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 15 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-83 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-83 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 3/09/2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

This is a response to Applicant's Amendments filed on June 15, 2007.

Claims 1-77 were originally pending. Claims 1, 4, 12, 20, 22, 28, 31, 34, 42, 50, 52, 58, 61, and 69 are amended. Claims 78-83 are newly added.

Claims 1-83 are now pending in the application.

### ***Response to Arguments***

1. Applicant's arguments, see Remarks, filed on June 15, 2007, with respect to the rejection(s) of claim(s) 1-77 under 35 USC 102(b) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of previously cited art, Sims III, in combination with prior art by Tai et al.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

Art Unit: 2132

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

1. Claims 1-21, 23-79, and 81-83 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Tai et al. [US Pub No. 2004/0034785 A1] hereinafter, Tai.

Based on independent claim 1, Sims III teaches an apparatus with a secure hard drive comprising a storage medium [6550011 B1, Col 13, Ln 4] that stores encrypted digital content and corresponding encrypted content keys [6550011 B1, Col 13, Ln 35]; a public key decryption module that receives one of said encrypted content keys from said storage medium and that decrypts said encrypted content key using a private key [6550011 B1, Col 12, Ln 1-4 – preselected device secret key] and generates a content key [6550011 B1, Col 11, Ln 50][ 6550011 B1, Col 17, Ln 62]; and a block decryption module that receives said encrypted digital content corresponding to said one of said encrypted content keys from said storage medium and said content key from said public key decryption module and that decrypts said encrypted content using said content key [6550011 B1, Col 11, Ln 50][ 6550011 B1, Col 18, Ln 5].

However, Sims III does not teach wherein said private key is generated based on a device specific identification (ID).

Tai teaches an encryption mechanism using unique chip die identification wherein a private key is generated based on a device specific identification (ID) [2004/0034785 A1, Pg 2, Par 0037 – a private random (cryptographic) key is generated using the unique 64-bit number based on the chip's die ID number.]

It would have been obvious to one of ordinary skill in the art at the time of invention to generate the private key of Sims III using the chip's die ID number as taught by Tai. The suggestion/motivation for combining would have been to generate keys without requiring knowledge about a key value [2004/0034785 A1, Pg 1, Par 0012]. Another would have been to generate a unique and unknown cryptographic key for each end product [2004/0034785 A1, Pg 1, Par 0014]. Sims III and Tai are analogous art because it solves the problem of generating a more secure private key.

With regard to dependent claim 2, the combined invention of Sims III and Tai teaches the secure hard drive of claim 1, where in said storage medium is a magnetic storage medium [6550011 B1, Col 13, Ln 5][Magnetic, per se, is inherent within the scope of writeable media].

With regard to dependent claim 3, the combined invention of Sims III and Tai teaches the secure hard drive of claim 1, wherein said public key decryption

Art Unit: 2132

module and said block decryption module are implemented by a system on chip (SOC) [6550011 B1, Col 14, Ln 12].

With regard to dependent claim 4, Sims III teaches the secure hard drive of claim 1 further comprising a content player that receives said decrypted digital content from said block decryption module and that generates at least one of an analog output signal and a digital output signal [6550011 B1, Col 6, Ln 52], and a public key decryption module [6550011 B1, Col 11, Ln 50 -- encryption/decryption engine] that uses a private key [6550011 B1, Col 12, Ln 1 -- device preselected secret key] to generate said content key based on said private key [6550011 B1, Col 12, Ln 20].

Sims III does not teach the secure hard drive further comprising: an identification ID module that provides said specific device ID, wherein said public key decryption module generates said private key using said device specific ID.

However, Tai teaches an identification ID module that provides specific device ID [2004/0034785 A1, Pg 2, Par 0033 -- encryption key registers holding the unique 64-bit chip die ID number], and wherein a hardware/firmware module [2004/0034785 A1, Pg 3, Par 0040] generates a private key using said device specific ID [2004/0034785 A1, Pg 2, Par 0037].

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the encryption/decryption engine, and add an identification ID module to Sims III's invention in order to extend its capability of generating a private key using the chip's die ID number as taught by Tai. The suggestion/motivation for combining would have been to generate keys without requiring knowledge about a key value [2004/0034785 A1, Pg 1, Par 0012]. Another would have been to generate a unique and unknown cryptographic key for each end product [2004/0034785 A1, Pg 1, Par 0014]. Sims III and Tai are analogous art because it solves the problem of generating a more secure private key.

With regard to dependent claim 5, the combined invention of Sims III and Tai teaches the secure hard drive of claim 1 further comprising a controller that performs buffer management and timing of read/write operations [6550011 B1, Col 13, Ln 5][Controllers performing buffer management and timing of read/write operations are inherent in writeable storage devices.]

With regard to dependent claim 6, the combined invention of Sims III and Tai teaches a system comprising the secure hard drive of claim 5 and further comprising an external host [6550011 B1, Col 20, Ln 8]; and a control interface that provides a communications interface between said controller and said

external host [6550011 B1, Col 20, Ln 48][A control interface is inherent to enable transfer of content as cited.]

With regard to dependent claim 7, the combined invention of Sims III and Tai teaches the system of claim 6, wherein said external host is one of a computer and a portable media player [6550011 B1, Col 19, Ln 30][6550011 B1, Col 20, Ln 8].

With regard to dependent claim 8, the combined invention of Sims III and Tai teaches the hard drive of claim 4 further comprising a watermark detector that communicates with an output of said content player and that determines whether said analog signal that is output by said content player contains a watermark [6550011 B1, Col 15, Ln 15].

With regard to dependent claim 9, the combined invention of Sims III and Tai teaches the secure hard drive of claim 1, wherein said storage medium stores a content directory having content directory entries for said content [6550011 B1, Col 19, Ln 6], [6550011 B1, Col 13, Ln 22].

With regard to dependent claim 10, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9, wherein said public key decryption module performs digital signature verification of said content directory entry



Art Unit: 2132

corresponding to said content that is selected for play [6550011 B1, Col 15, Ln 48][ 6550011 B1, Col 17, Ln 25].

With regard to dependent claim 11, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9 wherein at least one of said content directory entries contains a clear content counter that specifies a portion of said corresponding content that is not encrypted [6550011 B1, Col 15, Ln 7].

With regard to dependent claim 12, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9 wherein at least one of said content directory entries includes a content distributor ID field that identifies a content distributor supplying said corresponding content [6550011 B1, Col 13, Ln 25].

With regard to dependent claim 13, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9 wherein at least one of said content directory entries includes a content status field that has one of an active status and a passive status, wherein said active status enables playback and said inactive status disables playback [6550011 B1, Col 15, Ln 5].

With regard to dependent claim 14, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9 wherein at least one of said content

Art Unit: 2132

directory entries includes a signature field for said content distributor supplying said corresponding content [6550011 B1, Col 13, Ln 25].

With regard to dependent claim 15, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9 wherein at least one of said content directory entries includes a content key location field that contains a first offset value that points to a content key for said selected content in a content key block stored on said storage medium [6550011 B1, Col 13, Ln 22][Pointers as offset values are inherent in these data sets cited for the purpose of pointing to a content key.]

With regard to dependent claim 16, the combined invention of Sims III and Tai teaches the secure hard drive of claim 9 where in at least one of said content directory entries includes a content location field that contains a second offset value that points to said selected content in a encrypted content block stored on said storage medium [6550011 B1, Col 19, Ln 6][Pointers as offset values are inherent in a file system for the purpose of pointing to a selected content.]

With regard to dependent claim 17, the combined invention of Sims III and Tai teaches the secure hard drive of claim 1 wherein said content includes at least one of audio, video, and still pictures [6550011 B1, Col 7, Ln 62].

With regard to dependent claim 18, the combined invention of Sims III and Tai teaches the system of claim 6 further comprising a distributed communications network [Col 9, Ln 13]; and a content distributor that transmits encrypted content, an encrypted content key, and a content directory entry for a content selection to said secure hard drive via said external host and said distributed communications network [Col 20, Ln 2][A content distributor is inherent in a "pay per view" system.]

With regard to dependent claim 19, the combined invention of Sims III and Tai teaches the secure hard drive of claim 1, wherein said storage medium contains encrypted content that is pre-stored thereon [6550011 B1, Col 20, Ln 55].

Independent claim 20 is rejected using the same references as claims 1, 2, and 3.

Dependent claim 21 is rejected using the same reference as claim 4 with the limitation regarding a content player that receives said decrypted digital content.

Dependent claim 23, 24, 25, 26, and 27 are rejected using the same reference as claim 5, 6, 8, 9, and 10 respectively.

Art Unit: 2132

Dependent claim 28 is rejected using the same references as claims 11, 12, 13, 14, 15, and 16.

Dependent claim 29, and 30 are rejected using the same reference as claim 17, and 18 respectively.

Claims 31-49 are rejected using the same references as claims 1-19. Claims 1-19 is the apparatus with all limitations having the necessary structure and components as disclosed in the specification for performing the function recited in all the limitations of claims 31-49.

Claims 50-60 are rejected using the same references as claims 20-30. Claims 20-30 is the apparatus with all limitations having the necessary structure and components as disclosed in the specification for performing the function recited in all the limitations of claims 50-60.

Claims 61-77 are rejected using the same references as claims 1-6, 8-17, and 19. Claims 1-6, 8-17, and 19 is the apparatus with all limitations performing the method of claims 61-77.

Claim 78-79, and 81-83 are rejected because it contains the same subject matter as claim 4. [Chip ID is intrinsic to the device where the chip is being utilized.]

2. Claim 80 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US PN 6550011 B1], and further in view of Tai et al. [US Pub No. 2004/0034785 A1] and Heer et al [US PN 5999629].

Regarding claim 80, the combined invention of Sims III, and Tai teach the secure hard drive of claim 78, wherein said public key decryption module generates said content key based on a public key [US 6550011 B1, Col 12, Ln 17 – Content key is encrypted using device's public key, which is decrypted using device's secret key]. However the combined invention of Sims III and Tai do not teach wherein said public key decryption module generates a public key based on said private key.

Heer teaches a security module that generates a corresponding public key based from a device's private key [5999629, Col 4, Ln 34-51]

It would have been obvious to one of ordinary skill in the art at the time of invention to further modify the encryption/decryption engine of the combined invention of Sims III and Tai so that a corresponding public key can be generated from said private key. The suggestion/motivation for combining would have been to cover the device's secret key [5999629, Col 1, Ln 30-40] through the utilization of asymmetric cryptographic keys. Heer is analogous art because it solves the problem of not revealing the device's secret key in the communication channels.

Dependent claim 22 is rejected using the same reference as claim 80 because it contains the same subject matter since the public key is generated from the private key from which is generated using the Chip ID.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

Art Unit: 2132

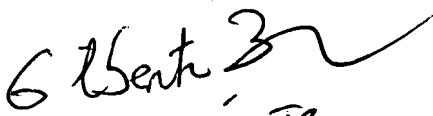
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan

Examiner. Art Unit 2132.

  
GILBERTO BARRÓN Jr  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100